INL/CON-07-13143
PREPRINT

Development of Standardized Probabilistic Risk Assessment Models for Shutdown Operations Integrated in SPAR Level 1 Model

PSAM 9

S. Khericha
J. Mitman

May 2008

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Development of Standardized Probabilistic Risk Assessment Models for Shutdown Operations Integrated in SPAR Level 1 Model

S. Khericha, Ph. D.[a*], J. Mitman[b]
[a]Idaho National Laboratory, Idaho Falls, ID, USA
[b]U.S. Nuclear Regulatory Commission, Washington DC, USA

Abstract: Nuclear plant operating experience and several studies show that the risk from shutdown operation during Modes 4, 5, and 6 at pressurized water reactors and Modes 4 and 5 at boiling water reactors can be significant. This paper describes using the U.S. Nuclear Regulatory Commission's full-power Standardized Plant Analysis Risk (SPAR) model as the starting point for development of risk evaluation models for commercial nuclear power plants. The shutdown models are integrated with their respective internal event at-power SPAR model. This is accomplished by combining the modified system fault trees from the SPAR full-power model with shutdown event tree logic. Preliminary human reliability analysis results indicate that risk is dominated by the operator's ability to correctly diagnose events and initiate systems.

Keywords: probabilistic risk assessment, shutdown, operating modes, outage

1. INTRODUCTION

The Idaho National Laboratory (INL) is in the process of developing shutdown probabilistic risk assessment (PRA) models for the U.S. Nuclear Regulatory Commission (NRC) to estimate the risk from shutdown operations. The shutdown models are built in the existing U.S. NRC full-power Standardized Plant Analysis Risk (SPAR) Level 1 model. References [1] and [2] provided the starting point for developing the event tree structure, plant operating state (POS) information, and other items specific to shutdown operations. Reference [1] delineates six technical specification operating modes for a pressurized water reactor (PWR) and breaks them down into 15 POSs. Reference [2], for a boiling water reactor (BWR) addresses the five technical specification operating modes with nine POSs. Modes 4, 5, and 6 for PWRs and Modes 4 and 5 for BWRs primarily require the residual heat removal (RHR) system. Core damage frequency was analyzed for only the one POS that significantly dominated the risk for each plant type. In the case of PWRs, this is the mid-loop operating state (POS 5); for BWRs, it is reactor coolant system (RCS) level normal until the vessel head is off (POS 4) (References 1 and 2).

In 2000, INL analysts developed an approach to estimate core damage frequency for shutdown operations. As stated in References [3] and [4], most of the risk from shutdown operations arises from Mode 4 (hot shutdown), Mode 5 (cold shutdown), and Mode 6 (refueling) for PWRs and Mode 4 (cold shutdown) and Mode 5 (refueling) for BWRs. The three PWR modes are further delineated into a total of 12 POSs based on the status of the primary system. It is implicitly assumed here that when a PWR transitions from Mode 3 to Mode 4, heat removal from the primary system switches from the steam generators to the RHR system. The two BWR modes are further delineated into a total of seven POSs based on the status of the primary system. These POSs were mapped into four time windows to characterize the shutdown operations. The time windows define average decay heat generation rate. A specific POS can be split into more than one time window. Although much of the data from References [1] and [2] were used, they were reformatted to accommodate an analysis based on technical specification defined operating modes.

In 2006, INL analysts further modified the analyses to integrate shutdown risk with internal and external events analyses. This changed the focus of the model from calculating only the overall risk integrated over a complete outage to a model that is also useful as an event or condition evaluation tool. Therefore, the emphasis on mapping of time window versus POS has been eliminated. In effect,

the model now calculates risk for a single time window for a given POS. An analyst can adjust the model for situations in which an extended timeline can have a significant effect on the operator action and consequently the level of risk.

Based on similar mitigating system applicability, the evolution of a plant outage has been delineated into nine POSs for PWRs and six POSs for BWRs. Only those plant configurations that rely primarily on the RHR system for removal of primary system decay and residual heat are included in this analysis. These mode-based plant operating states are described in the next section. This shutdown model is constructed using the system fault tree models, common cause failure modeling, and most of the basic event definition and quantification from the full-power SPAR model.

2. SPAR MODELS AND THE SAPHIRE CODE

PRA use has significantly increased in the NRC regulatory framework of the U. S. nuclear power industry. For this purpose, INL has developed a set of 75 plant-specific SPAR models to provide critical risk-based input to the regulatory process. The models use a linked fault tree construction methodology and results are calculated using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) quantification code. SAPHIRE is a powerful, personal computer software application for performing PRAs [5]. Using SAPHIRE, an analyst can perform a PRA for any complex system, facility, or process. For nuclear power plants, SAPHIRE can be used to model a plant's response to initiating events, quantify associated core damage frequencies, or identify important contributors to core damage The models are standardized in their quantification software, failure data used [6], human reliability methodology [7], modeling detail level, and naming rules.

3. CHARACTERIZATION OF PRESSURIZED WATER REACTOR SHUTDOWN OPERATIONS

The set of POSs selected for inclusion in the shutdown SPAR models were defined in an analysis of the transitions and configurations associated with plant shutdown, outage, and startup operations. Naming conventions similar to those used in References [3] and [4] have been followed, and can be used to associate event trees, fault trees, and basic events with a particular initiating event and plant state. The POS names are based on a six-character identifier that defines five POS characteristics:

- Plant mode
  - M4 Mode 4
  - M5 Mode 5
  - M6 Mode 6
- Time frame (in relation to refueling mode)
  - E Early (before refueling)
  - L Late (after refueling)
  - X Not applicable (refueling mode)
- Pressure (not applicable to PWR)
  - L Low or atmospheric
  - H Hydro test
- RCS inventory status

PWR:		BWR:	
R	Reduced RCS inventory	N	Normal RCS inventory
F	Full RCS inventory	S	Steam-line RCS inventory
C	Cavity flooded	U	Cavity flooded

- RCS pressure boundary status (not applicable to BWR)
  - V Vent open in the RCS pressure boundary
  - I Intact RCS pressure boundary
- RCS loop status (not applicable to BWR)
  - B Blocked RCS loops (i.e., all steam generators are isolated from the rest of the RCS)
  - O Open RCS loops (i.e., RCS flow through the steam generators is possible).

The fraction of time spent in any POS (and whether it is entered at all) is related to the type of outage being undertaken. Table 1 lists the 15 overall POSs for PWRs with the corresponding identifiers used in the SPAR models. Table 2 lists the POSs and SPAR identifiers for BWRs.

4. MODEL ASSUMPTIONS

The current low power and shutdown SPAR model focuses on plant operating Modes 4, 5, and 6 for PWRs and Modes 4 and 5 for BWRs. The initiating events included in the model are the loss of RHR (failures and isolations of RHR are considered separately), loss of inventory (from the creation of openings or flow diversions in the RCS), loss of level control while at reduced inventory conditions, over-draining events, and both partial and full losses of offsite power. The SPAR model does not include reactivity control issues, cold over-pressurization issues, spent fuel pool events, or fuel-handling accidents.

There are five important areas where analysts should be aware of modeling assumptions made in development of the SPAR model for shutdown evaluations:

- Model success criteria
- "Weighted-average" fractions for time spent in various POSs
- Test and maintenance baseline assumptions
- Human error probabilities
- Definition of core damage.

There can be a lack of consensus on the success criteria for providing adequate heat removal during shutdown. This problem makes it difficult to unambiguously model shutdown configurations. Some of the methods for providing decay heat removal (such as reflux cooling and gravity feed) are rarely, if ever, tested or used and there is little known about the plant operators' understanding and training concerning the actual implementation of these methods of RCS heat removal.

The configurations that are allowable during shutdown operation and the amount of time spent in each vary significantly between plants and even between outages at any given plant. Data are lacking for important factors that affect shutdown core damage frequency such as the fraction of time spent in a mid-loop configuration. Another question without a clear answer is the fraction of time that secondary cooling is viable because of constraints such as the existence of an opening in the RCS pressure boundary that cannot be readily closed in response to an emergency. Test and maintenance unavailability are also important in calculating core damage frequency but sufficient data to characterize them accurately are currently not available. Identifying equipment that is out-of-service but can be rapidly put into service also appears to be a significant issue that is not explicitly addressed in the model. These issues are critical when calculating an average outage risk. When calculating risk from a specific outage or from an actual event occurring in a specific outage, these issues are resolved by using outage specific data.

Human error is another important consideration. Evaluation of the factors that may increase the likelihood of operator error during a particular condition is hampered by the limited information and analyses performed to date. The SPAR shutdown-related human error probabilities in the model were generated through SAPHIRE's built-in human reliability analysis (HRA) code [5].

Recovery of failed equipment also is not universally included in the model. Some system fault trees (which for the most part are taken directly from the corresponding full-power SPAR model) include a generalized recovery event obtained from actual operating experience data for full-power operations.

Another important aspect in characterizing shutdown risk is the decay heat level. To account for the various levels of decay heat, the SPAR shutdown models define four time windows in terms of time after reactor shutdown (see Table 3).

Table 1: PWR Operating States and Corresponding Modes and SPAR Descriptions [1]

Plant Operating State	POS Description	Technical Specification Mode	SPAR Description[a]
POS 1	Low power and reactor shutdown	Power Operation	NA
POS 2	Cooldown with steam generators from operating temperature to 345°F	Hot Standby	NA
POS 3	Cooldown with RHR from 345 to 200°F	Hot Shutdown	M4EFIO
POS 4	Cooldown with RHR (below ≈200°F)	Cold Shutdown	M5EFIO
POS 5	Draining RCS to mid-loop	Cold Shutdown	M5ERIO MERVB
POS 6	Mid-loop operation	Cold Shutdown	
POS 7	Fill for refuelling	Cold Shutdown	
POS 8	Refueling	Refueling	M6XCVB
POS 9	Draining RCS to mid-loop after refueling	Cold Shutdown	M5LRIO MLRVB
POS 10	Mid-loop operations after refueling	Cold Shutdown	
POS 11	Refilling RCS	Cold Shutdown	
POS 12	RCS heatup solid and draw bubble	Cold Shutdown	M5LFIO
POS 13	RCS heatup to 350°F	Hot Shutdown	M4LFIO
POS 14	RCS heatup with steam generators available (above 350°F)	Startup	NA
POS 15	Startup and low power operations	Power Operation	NA
a. NA is not applicable.			

Table 2: BWR Operating States and Corresponding Modes and SPAR Descriptions [2]

Plant Operating State	POS Description	Technical Specification Mode	SPAR Description[a]
POS 1	Power operation	Power Operation	NA
POS 2	Startup; mode switch in startup/hot standby	Hot Standby	NA
POS 3	Mode switch in shutdown, plant temperature greater than 200°F	Hot Shutdown	NA
POS 4	Mode switch in shutdown, plant temperature ≈200°F or lower, low pressure, normal water level	Cold Shutdown	M4ELN[b]
POS 5	Mode switch in shutdown, plant temperature ≈200°F or lower, head off, low pressure, water level at the main steam lines	Cold Shutdown	M5ELS
POS 6	Mode switch in shutdown, plant temperature ≈200°F or lower, low pressure, cavity flooded	Cold Shutdown	M5XLU
POS 7	Mode switch in shutdown, plant temperature ≈200°F or lower, low pressure, water level at the main steam lines	Cold Shutdown	M5LLS
POS 8	Mode switch in shutdown, plant temperature ≈200°F or lower, low pressure, normal water level	Cold Shutdown	M4LLN
POS 9	Mode switch in shutdown, plant temperature ≈200°F or lower, high pressure, normal water level	Cold Shutdown	M4LHN
a. NA is not applicable.			

Table 3: Time Window Definitions for PWRs

Condition	Time Window 1	Time Window 2	Time Window 3	Time Window 4
Plant Operating States PWR	M5ERIO M5ERVB	M4EFIO M5EFIO M5LRIO M5LRVB	M4LFIO M5LFIO	M6XCVB
Average Time to Boil Off (before RHR is tripped or isolated)	15 min	30 min	90 min	>3 hr

5. EVENT TREE MODELS

The event trees are organized in a hierarchal fashion, with the single initial event tree determining the specific POS. Figures 1 through 6 show example event trees for a PWR. Figure 1 begins with the assumption that the plant is shut down (i.e., Mode 4 [hot shutdown], 5 [cold shutdown], or 6 [refueling]). The end states of the shutdown event tree delineate the nine POSs that result from the analysis. Figure 2 is similar but shows a BWR beginning with the assumption that the plant is in Mode 4 (hot shutdown) or Mode 5 (cold shutdown and refueling). Each POS then transfers to a second-level event tree (Figure 3) that accounts for the likelihood of each of the seven initiating events occurring, given a particular POS. Each of these second-level event tree end states then transfers to a third-level event tree (Figure 4) specifically tailored to the initiating event and includes initiating event-specific diagnosis and recovery functions. The initiating event- and POS-specific details are captured in the event tree logic rules (e.g., steam generators are not available for cooling). Finally, each initiating event tree transfers to two plant response trees that model the responses of the RHR and emergency core cooling systems (Figures 5 and 6).

Note that the shutdown event tree is not linked logically with the rest of the event trees. It is linked only by the conditional probabilities that it generates for its various end states. In other words, the shutdown tree can be quantified to generate conditional probabilities for being in the nine POS end states. Those conditional probabilities can then be used as event probabilities when quantifying any or all of the nine POS-specific event trees.

6. HUMAN RELIABILITY ANALYSIS

Because of the very limited number of automatic equipment actions that are typically functional during shutdown, operator actions are more dominant during shutdown than during at-power conditions. The shutdown SPAR models use the SPAR-H methodology [7]. The SPAR-H method is straight forward, easy to apply, and is based on a human information processing model and results from human performance studies available in the behavioral science literature.

As with any simplified method, SPAR-H has modeling and analysis limitations. SPAR-H identifies eight performance shaping factors (PSFs) capable of influencing human performance: available time, stress and stressors, experience and training, complexity, ergonomics, procedures, fitness for duty, and work process. Traditionally, accounting for the influence of multiple shaping factors with multiple levels of influence without imposing a high degree of expert consensus judgment on the HRA process has proven difficult. Ultimately, the analyst's expertise and judgment comes into play in assigning the correct level of PSF, particularly in the scenarios where there is no significant time available to diagnose the failures and recover from it.

In addition, because of the large numbers of sequences that contain multiple human error probabilities, HRA dependency analysis is critical to realistic shutdown analysis. Finally, many of the sequences take many hours to lead to core damage leaving significant time for operators to perform required tasks. SPAR-H, as with all HRA methods, does not supply good guidance on dealing with these issues. The project continues to refine this area of analysis.

7. TYPICAL RESULTS

Table 4 lists the preliminary conditional core damage probabilities of an initiating event occurring while the plant is in a particular POS. As expected, a majority of the risk is during reduced inventory operations. However, this risk is dominated by the operator actions, such as failure to diagnose or initiate the systems in time.

Figure 1: A First-Level PWR Shutdown Event Tree

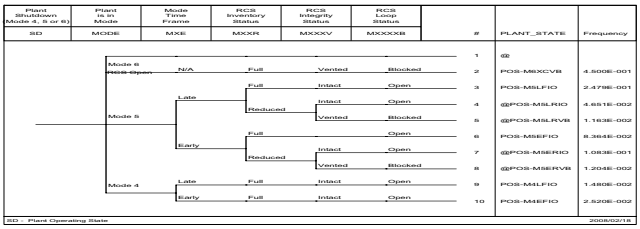

Figure 2: A First-Level BWR Shutdown Event Tree

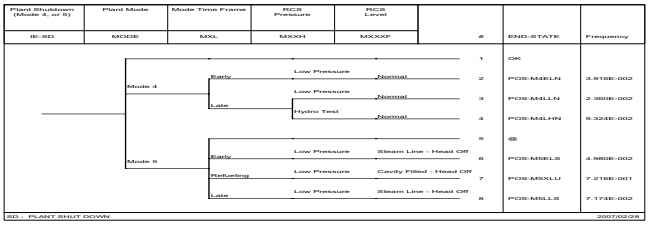

Figure 3: A Second-Level PWR Event Tree (M4EFIO)

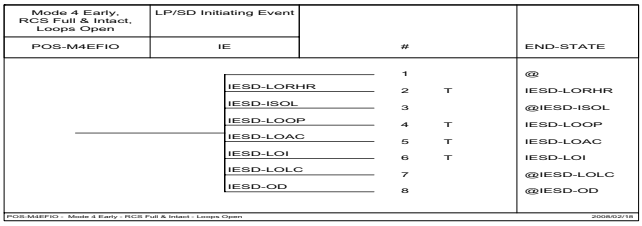

Figure 4: A Third-Level PWR Event Tree (Loss of Inventory)

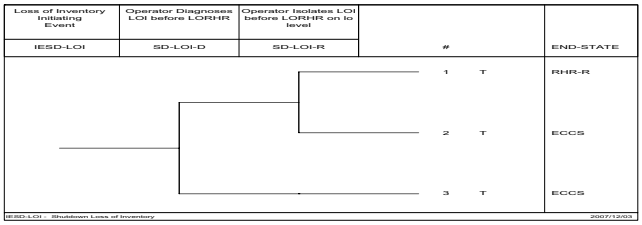

Figure 5: A PWR Restoration of RHR Cooling Event Tree

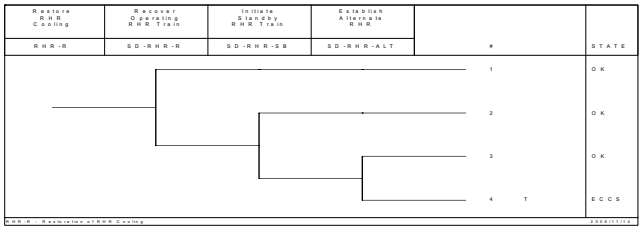

Figure 6: A PWR ECCS Inventory Control Event Tree

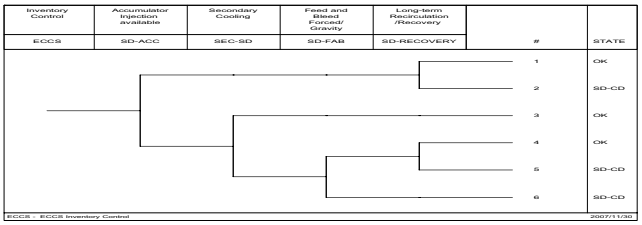

Table 4: Conditional Core Damage Probability for PWR Shutdown Operations

		Probability per Hour per Initiating Event						
POS	**POS Description**	**ISOL[1]**	**LOAC[2]**	**LOI[3]**	**LOLC[4]**	**LOOP[5]**	**LORHR[6]**	**OD[7]**
M4EFIO	Mode 4 Early RCS Full & Intact, Loops Open	7.3E-09	3.9E-08	1.4E-10	0.0E+00	1.3E-09	6.4E-09	NA
M4LFIO	Mode 4 Late RCS Full & Intact, Loops Open	7.3E-09	3.9E-08	1.4E-10	0.0E+00	1.3E-09	6.4E-09	NA
M5EFIO	Mode 5 Early RCS Full & Intact, Loops Open	7.3E-09	3.9E-08	1.4E-10	0.0E+00	1.3E-09	6.4E-09	NA
M5ERIO	Mode Early RCS Reduced & Intact, Loops Open	6.1E-05	3.0E-05	1.0E-05	9.7E-08	5.0E-06	5.3E-05	5.4E-06
M5ERVB	Mode Early RCS Reduced & Vented, Loops Blocked	5.1E-05	4.1E-05	8.3E-05	8.1E-08	4.7E-06	4.5E-05	4.5E-06
M5LFIO	Mode 5 Late RCS Full & Intact, Loops Open	7.3E-09	3.9E-08	1.4E-10	0.0E+00	1.3E-09	6.4E-09	NA
M5LRIO	Mode 5 Late RCS Reduced & Intact, Loops Open	7.3E-09	3.9E-08	4.4E-08	2.1E-10	1.3E-09	6.4E-09	1.1E-08
M5LRVB	Mode 5 Late RCS Reduced & Vented, Loops Blocked	3.2E-06	2.3E-05	4.4E-05	8.1E-08	7.9E-07	2.8E-06	4.5E-06
M6XCVB	Mode 6 RCS Full & Vented, Loops Blocked	1.5E-08	6.1E-07	1.6E-09	0.0E+00	1.4E-08	1.4E-08	NA

Notes:
1. Isolation of the primary means of shutdown cooling, typically RHR, from closure of a hotleg isolation valve.
2. Loss of alternating current power only to the running RHR train.
3. Loss of RCS inventory typically due to valve misalignment.
4. Loss of level control during reduced inventory (this is a short-term level decrease necessitating a shutdown of RHR without a loss of inventory).
5. Loss of offsite power.
6. Loss of the running RHR loop—not covered by the other initiators.
7. Overdrain—failure to terminate the drain down to mid-loop when desired level is reached (this is the only per demand initiator).

8. SHORTCOMINGS IN SHUTDOWN PROBABILISTIC RISK ASSESSMENT

The initiating events used in the shutdown models are derived from those provided in References [3] and [4]. An initiating event in the context of this report is an event that results in a loss of the operation shutdown cooling loop such that there is either a 15°F temperature rise or a mode change (i.e., temperature rises above 200°F). Events that satisfy this criterion were extracted from NRC licensee event reports and entered into a stand-alone database for use in estimating initiating event frequencies for shutdown. The criterion of 15°F temperature rise is rather arbitrary. There were significant numbers of events that resulted in loss of RHR but recovered in a very short time. No specific data are available on other initiating events during shutdown. Additional research is currently underway to expand these data to include all losses of RHR without a temperature increase restriction.

During full-power operation, many safety systems are tested regularly. However, during shutdown, scheduled testing of a component or system depends on the POS and plant procedures. For example, a non-operating RHR train and its support systems cannot be taken down for scheduled test and maintenance while operating in reduced inventory POS. However, there is a very high likelihood that one RHR train will not be available when a cavity is flooded because it is out for test and maintenance. Because of these considerations, the normal test and maintenance terms in the at-power models are not used in the shutdown models. Instead, the analyst is required to include actual

equipment unavailability during event analysis. Also, the time available for operator actions for recovery depends on the POS of the plant. There are no data on mean time to repair or recover from scheduled or forced maintenance during shutdown operations.

9. CONCLUSION

Because of the very limited number of automatic equipment actions that are typically functional during shutdown, operator actions are more dominant during shutdown than during at-power conditions. The risk is dominated by the operator's understanding of the event and the ability to respond appropriately. In the example PWR, more than 98% of the core damage frequency was dominated by operator actions. Several core damage cutsets include three or more operator actions. Therefore, understanding and modeling dependency of operator actions is a very important aspect of the total risk. Based on this analysis of PWRs, the risk to fuel damage (per hour) during shutdown operations is comparable to at-power operations.

Acknowledgements

The authors acknowledge the support of Selim Sancaktar of the NRC, who provided many of the technical suggestions, and Dan Henry, Bob Buell, and John Schroeder of the INL who provided much guidance in the development of these models. The authors also express their appreciation to Erulappa Chelliah, Bennett Brady, and Mike Cheok, NRC staff who encouraged us to publish this manuscript.

References

[1] T. L. Chu et al. *Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1—Analysis of Core Damage Frequency from Internal Events During Mid-Loop Operations, Vol. 2*, NUREG/CR-6144, June (1994).
[2] D. Whitehead et al. *Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf Unit 1—Analysis of Core Damage Frequency from Internal Events for Plant Operational State 5 During a Refueling Outage, Vol. 2*, NUREG/CR-6143, June (1994).
[3] D. Henry et al. *Low Power and Shutdown Operation Standardize Plant Analysis Risk Model Template for BWRs*, Unpublished Report, September (2004).
[4] W. Galyean et al. *Low Power and Shutdown Operation Standardize Plant Analysis Risk Model Template for PWRs*, Unpublished Report, August (2002).
[5] K. D. Russell et al. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0*, NUREG/CR-6116, (1993).
[6] S. A. Eide et al. *Industry-Average Performance for Components and Initiating Events at U. S. Commercial Nuclear Power Plants*, NUREG/CR-6928 (INEEL/EXT-04-11119), January (2007).
[7] D. Gertman et al. *The SPAR-H Human Reliability Analysis Method*, NUREG/CR-6883 (INEEL/EXT-05-00509), August (2005).